VOLUME 2, ISSUE 3

OCTOBER 2009

InsighT to Security

State of Idaho, Office of the CIO, Cyber Security Newsletter

In this Issue:

All About Cybercrime (from MS-ISAC)

What is Cybercrime?

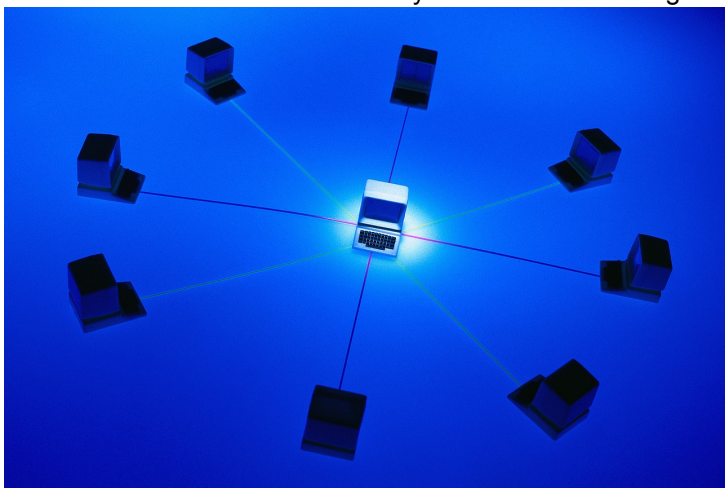
The term "cybercrime" is usually referred to as any criminal offense committed against or with the use of a computer or computer network. The US Department of Justice (DOJ) interchangeably uses the terms "cybercrime," "computer crime," and "network crime" to refer to acts such as computer intrusions, denial of service attacks, viruses and worms.[1] A cybercrime incident can lead to loss of business and consumer confidence, financial loss, productivity loss, and even loss of intellectual property. For something to be considered a crime, however, requires a law to denote it as such, and the laws have, to this point, lagged behind technology. Existing laws relating to cybercrime oftentimes do not apply to specific acts being investigated and those laws vary from state to state. Some cybercrime may be more easily prosecuted if it is simply viewed as a more commonly recognized crime, e.g. vandalism instead of web defacement. To refer to a criminal act as "cybercrime" or "computer crime" tends to place the focus more on the technology, rather than on the crime itself. For these reasons, Anthony Reyes, author of the book *Cyber Crime Investigations*, argues against using the term "cybercrime," and instead prefers to

Cybercrime (from page 1)

call these acts as "crimes with a computer component."[2] Regardless of the means used to commit a crime or the target of a crime, whether it is a computer, a business, or someone's data, it is still a crime.

What are the Trends in Cybercrime?

In the 1990s, cybercrime was mainly motivated by notoriety or revenge and predominately defined by the willful destruction of online property or intentional disruption of a business. The current era of cybercrime is dominated by criminals who want to use your computer for illegal activities, to steal data for profit, and organized crime is heavily involved.[3] Attackers exploit vulnerabilities in computer software in order to develop "crimeware," such as viruses, Trojans, and keyloggers, in order for other criminals to carry out their nefarious acts. These "crimeware" creators also utilize the software-as-a-service business model to provide crimeware-as-a-service. Some of their crimeware servers not only act as command and control servers (machines designed to provide instructions to the crimeware), but also as "data suppliers" or repositories for private stolen information that is harvested by the crimeware. Personal information is a valuable commodity for criminals. Traditional security tools are becoming increasingly more limited in their ability to mitigate these highly complicated cybercrime attacks.[4] Another trend is that the governments of various countries are suspected of being involved in cybercrimes for political reasons. As governments become more dependent upon technology, those assets will be attacked for various reasons. The cybercrime landscape, as it may be called, has definitely changed, but the criminal motivations are still the same – money, power and revenge.



What Can I Do?

Fighting cybercrime is problematic for several reasons. Many actions, such as writing crimeware, are currently not defined as illegal and, even if they constitute a crime, can be difficult to prosecute. Location and jurisdiction may also be a problem. For instance, a criminal may reside in one country and use a crimeware server in another country to attack a victim who resides in a third country.[5] Cybercrime can also be perpetrated without a person's knowledge, unlike other types of crimes that may be more noticeable. To adequately defend against cybercrime, you need against cybercrime, you need to follow the traditional best practices for protecting your network or desktop.

If you become a victim of cybercrime, you should report the incident to the appropriate law enforcement authorities. Depending on the scope of the crime, the appropriate agency may be local, state, federal, or even international. The US DOJ maintains a list of federal agencies to which computer related crimes may be reported at the following address: http://www.usdoj.gov/criminal/cybercrime/reporting.htm.

In addition, you may report cybercrimes to the Internet Crime Complaint Center (IC3), a partnership among the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA). The IC3 provides a convenient reporting mechanism for both citizens and government agencies that alerts authorities of suspected criminal or civil violations and may be contacted via the following address: http://www.ic3.gov.

Cyber Security Awareness Month—October

October: Governor signs Proclamation

October 1: Boise Information Systems Security Association Monthly Meeting—Boise, ITT Tech

Business Continuity, Disaster Recovery, and Risk Analysis Round-Table.

October: Press Release distributed for media utilization

Simple news release, describing the purpose of the Cyber Security Awareness Month, distributed through out the state's media.

October: Security Awareness Presentations—Boise, Idaho Transportation Department Auditorium

Presentation on our vulnerability to Cyber threats, the current trends of security incidents, and what we can do to protect ourselves. These are designed for state employees, but all citizens of Idaho are welcome and encouraged to attend.

Date	7 October	9 October	21 October	22 October	28 October	29 October
Time 1	8:00-9:00 am	2:00-3:00 pm	9:00-10:00 am	9:00-10:00 am	1:00-2:00 pm	1:00-2:00 pm
Time 2			10:30-11:30 am	10:30-11:30 am	2:30-3:30 pm	

October 8: National Cyber Security Awareness Webcast—"Our Shared Responsibility—The Strategy for Promoting Cyber Security Awareness—On-Line

October 15: University of Idaho, Computer Security Awareness Symposium - 2009—Moscow, U of I

University of Idaho's annual Information Technology Service's Computer Security Awareness Symposium, Idaho Commons Clearwater Room; http://support.uidaho.edu/csas2009/

October 17: Cyber security awareness posters and guides distributed to state & local agencies and businesses

October 29: BSU, Info Sec Office's Personal Information Security Event—SUB, Alexander Ballroom

Promoting awareness of IT Security for the BSU Student body and visitor

Office of the CIO, Cyber Security Newsletter

650 W State St
Boise ID 83720

Phone: 208-332-1851
Email: terry.pobst-martin@cio.idaho.gov

CHECK OUT THESE LINKS

Security Websites:

Good websites to surf:

http://www.sans.org/

http://www.cert.org/

http://www.msisac.org/

http://csrc.nist.gov/

http://www.issa.org/

http://www.infragard.net/

http://www.ic3.gov/

http://www.securityfocus.com/

http://www.snopes.com/

http://www.nationalterroralert.com/

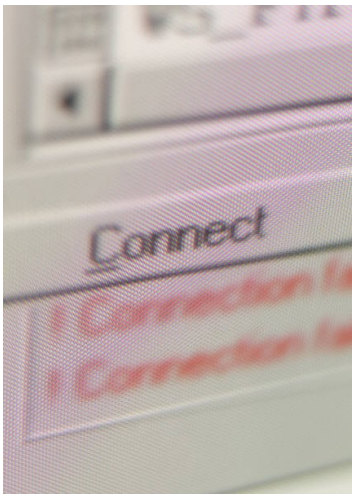
If you act defensively on the internet, you'll be safer.

Just like driving defensively, you should browse defensively. Watch out for the bad guys!

Quick Security Highlights

September 30, from *IT Pro* – Symantec reported new botnet players are emerging since a shut-down of ISPs hosting botnet activity in the last year. Botnets are now responsible for sending 87.9 percent of all spam; a newer botnet called Maazbem is growing rapidly. In May Maazbem spewed out casino-related spam emails. Maazben's growth has accelerated over the past month, from 0.5 percent of all spam in August to 1.4 percent of all spam in September. A MessageLabs Intelligence senior analyst said in a statement that the number of ISPs being taken offline for hosting botnet activity had resulted in a case of older botnets sinking and newer botnets taking their place. He said: "This has undermined the power of the more dominant botnets like and cleared the way for new botnets like Maazben to emerge." However, one of the oldest and largest botnet, Rustock, has doubled in size since June - it is the only botnet to have a regular spam cycle.

September 30, from the *Washington Post* – Hackers last week apparently used stolen account information from a New Jersey company that provides online payroll services to target the firm's customers in a scheme to steal passwords and other information. The New Jersey-based PayChoice provides direct payroll processing services and licenses its online employee payroll management product to at least 240 other payroll processing firms, serving 125,000 organizations. Last Wednesday, a number of PayChoice customers received an e-mail warning them that they needed to download a Web browser plug-in in order to maintain uninterrupted access to onlineemployer.com, the portal for PayChoice's online payroll service. The supposed plug-in was instead malicious software designed to steal the victim's user names and passwords. In a statement e-mailed to Security Fix, PayChoice said the company discovered on September 23 that its online systems had been breached. The company said it immediately shut down the onlineemployer.com site and instituted fresh security measures to protect client information, such as requiring users to change their passwords. PayChoice said the malicious sites downloaded a Trojan horse program called TrojanDownloader:Win32/Bredolab.X, which is a malware program that tries to download additional malicious files and disable security software on the infected PC.

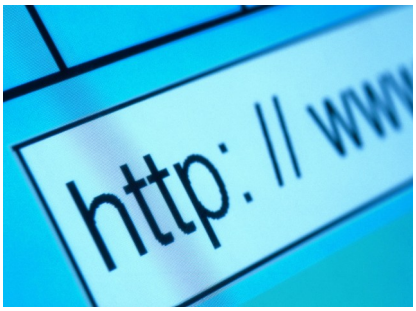


What Are Browser Cookies?? (from MS-ISAC)

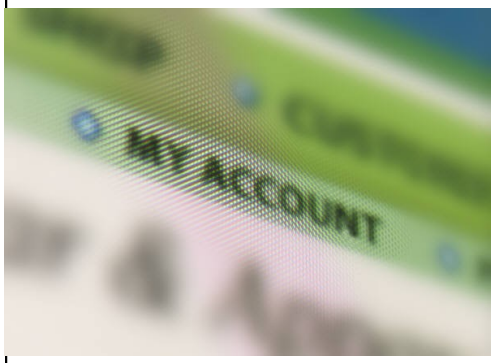
Did you know you can get "browser" cookies almost every time you go on the Internet? These cookies help with Internet commerce, allow quicker access to web sites, or can personalize your browsing experience. However, there are some privacy and security issues to be aware of, so it is important to understand the purpose of a browser cookie and manage their use on your computer appropriately. This tip will help you understand what a browser cookie is, what it is used for and what risks might be associated with using cookies.

What's a Browser Cookie and How is it Used?

Browser cookies are simply reference files stored on your computer, just like pictures and documents. When you visit a web site, the visited web site will often place a cookie on your computer. Cookies do not contain active content (executables) or links, just text-based information. The information in the cookie might indicate how often you visit the site, what kind of products you bought, what kind of things you searched for, etc.

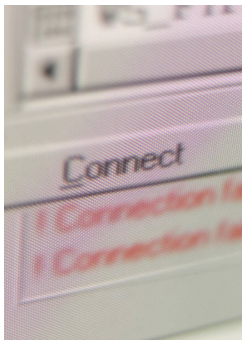


There are two different types of browser cookies that are stored on your computer – session and permanent cookies. Session cookies are stored in the computer's memory only during your browsing session and are automatically deleted from your computer when the browser is closed. These cookies usually store a session ID that is not personally identifiable, allowing you to move from page-to-page without having to log-in repeatedly. Session cookies are never written to the hard drive and they do not collect any information from your computer. They are widely used by commercial web sites; for example, to keep track of items that a consumer has added to a shopping cart. For instance, when you add an item to your shopping cart while shopping online, the information on that item is placed into a cookie. When you are finished with your online shopping, the application then references the appropriate cookie, tallies up your purchases, and bills you for those items.



Permanent cookies are stored on your computer's hard drive and are not deleted when the browser is closed. These cookies can retain user preferences for a particular web site, allowing those preferences to be used in future browsing sessions. Permanent cookies can be used to identify individual users, so they may be used by web sites to analyze users' surfing behavior within the web site. These cookies can also be used to provide information about number of visitors, the average time spent on a particular page, log-in information stored in an account, and generally the performance of the web site.

In addition to session and permanent cookies, many sites allow their advertisers to place "third-party" cookies on your computer. Third-party cookies allow the marketing or an advertising company to track your interests and browsing through multiple web sites and companies. Third-party cookies, ones used by companies you are not dealing directly with, are more of a privacy issue than a security issue. The more you allow companies to track your online behavior, the more they can market directly to your specific interests. How cookies are processed and/or stored on your computer is controlled by your browser's privacy settings.



Risks and What Should I Do?

Although permanent cookies may be useful and convenient, there are risks associated with stored log-in credentials. Storing credentials in a cookie can increase the risk of your log-in information being discovered if someone else uses your computer or in the event your computer may be compromised. If your computer or the website you are visiting is compromised, cookies can be used for malicious purposes, such as hackers altering data in the cookie or intercepting traffic between your computer and the web site.

Is recommended that you:

- Set your cookie preferences using your browser privacy settings.
- Periodically delete cookies from your computer.
- Session cookies should be automatically deleted when you have completed a financial transaction online. By clearing your cookies from your browser periodically you can decrease the risk of the misuse of information accidentally or intentionally stored in cookies.
- Do not allow cookies to store login information.
- Keep your system and browser up-to-date on patches, update your anti-spyware software, and only visit trusted web sites.
- If you do not want to share your online behavior data with third-parties, set your privacy settings to not allow third-party cookies. Note, this may impact your browsing experience.
- Be cautious when sharing your computer. If you stored credential information using a browser cookie (user names and password), the individual using your computer will have access to your account and will be able to process transactions in your name.

For More Information on Cookies Visit:

Web Browser Attacks: www.msisac.org/awareness/news/2008-07.cfm
Browsing Safely: Understanding Active Content and Cookies: www.us-cert.gov/cas/tips/ST04-012.html
Evaluating Your Web Browser's Security Settings: www.us-cert.gov/cas/tips/ST05-001.html
Http Cookie: http://en.wikipedia.org/wiki/HTTP_cookie
Free Security Checks: www.staysafeonline.info/content/free-security-check-ups
How to Control Cookies: www.aboutcookies.org/Default.aspx?page=1